Install Tails from Windows

tails.net/install/windows

You need

1 USB stick

Only for Tails!

8 GB minimum

Your primary Tails

1 USB stick

All data will be lost!

8 GB minimum

Why?

It is currently impossible to manually upgrade a Tails USB stick while running from itself. This scenario requires creating an intermediary Tails on another USB stick, from which to upgrade your Tails.

Windows 8

or later

macOS 10.10

Yosemite or later

Linux

any distribution

Debian

Ubuntu

or another derivative

Another Tails

USB stick or DVD

2 GB of RAM

64-bit

Intel processor

not Apple processor

2 GB of RAM

64-bit

Smartphone

or printer to follow the instructions

1 hour in total

½ hour

¼ hour

1.8 GB to download

½ hour to install

½ hour to upgrade

To learn about the processor in your Mac, choose **Apple menu ▸ About This Mac** and check the **Processor** or **Chip** information.

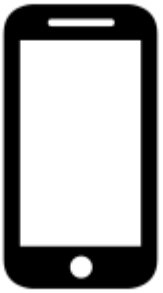
If your Mac has an Apple chip, Tails won't work.

Making Tails work on Apple chips represents a massive engineering challenge.

The Asahi Linux project is working on support for Apple chips in Linux. Support for Apple chips in Debian is following along, but it is not complete yet.

You can track our own experiments on #10972.

System requirements and recommended USB sticks



System requirements

Tails works on most PC computers that are less than 10 years old.

Tails does not work on:

- Mac computers with an Apple processor (M1, M2, and so on)
- Smartphones or tablets
- Raspberry Pi

Tails might not work on some PC computers, for example, if their graphics card is incompatible with Linux. Nvidia or AMD Radeon cards often do not work in Tails.

See our list of known hardware compatibility issues.

Detailed hardware requirements

- 3 GB of RAM to work smoothly.

  Tails can work with less than 3 GB RAM but might experience reduced performance, instability, or crashes.

- The ability to start from a USB stick or a DVD reader.

- A 64-bit x86-64 IBM PC compatible processor.
    - Tails does not works on ARM or PowerPC processors.
    - Tails does not work on 32-bit computers since Tails 3.0 (June 2017).

Recommended laptops

Laptop models evolve too rapidly for us to be able to provide an up-to-date list of recommended hardware. Below are some guidelines if you, or your organization, are considering acquiring a laptop dedicated to running Tails.

For PC

- Avoid "gaming" models with Nvidia or AMD Radeon graphics cards.
- Consider buying a refurbished laptop from a high-end (professional) series. These are cheaper and will last longer than new but lower-quality laptops.
    - For example, the Lenovo ThinkPad series work well with Tails, including the X250, X1 Carbon, T440, T480, and T490 models.
    - If you live in a part of the world where buying refurbished laptops is uncommon, look on eBay and Amazon. Amazon offers a 90-day Amazon Renewed Guarantee.
- Consider buying a new laptop from vendors who guarantee the compatibility with Linux and Tails like ThinkPenguin.

For Mac

Tails still works on some older Mac computers with an Intel processor.

Unfortunately, we don't know of any Mac model that works well in Tails and can run the latest macOS version.

Recommended USB sticks

You need a USB stick of 8 GB minimum to use Tails.

All the data on this USB stick is lost when installing Tails.

The quality of your USB stick is crucial when using Tails. A bad USB stick will be slower and more likely to corrupt the files in your Persistent Storage.

We recommend that you:

- **Buy new USB sticks.**

  USB sticks become slower and less reliable over the years. Older USB sticks were also built with slower technology.

- **Buy USB sticks from well-known brands, such as Kingston, Samsung, and SanDisk.**

  Generic brands are more likely to be slower and less reliable.

  Any modern USB stick from a well-known brand is fast enough to use Tails comfortably.

- **Buy your USB sticks from a reputable local store.**

  If you are in a place where counterfeit electronics are common, buy your USB stick from an international supermarket chain, which should have a more reliable supply chain.

  Avoid buying USB sticks online or using USB sticks that were given to you, because they could contain malware.

- **Consider buying faster USB sticks that support USB version 3.0 or later.**

  Check the specifications of your computer to determine whether your USB ports support USB 3.0 or later. USB 3.0 ports are sometimes blue.

  USB 3.0 can be up to 10 times faster than USB 2.0. USB 2.0 has a maximum read speed of around 50 MB/s on USB sticks, while USB 3.0 has a maximum read speed of around 500 MB/s.

  Most quality USB sticks nowadays have read speeds of at least 100 MB/s and are faster when used on USB 3.0 ports. Some USB sticks advertised for USB 3.0 have even greater speeds.

  You can test the write speed of your different USB sticks by comparing the time it takes to clone Tails, for example.

How many USB sticks should I buy?

If you want to store personal files and configuration in an encrypted Persistent Storage, we recommend that you buy 2 USB sticks, ideally 3:

- 1 USB stick to be your **primary Tails**.

Warnings: Tails is safe but not magic!

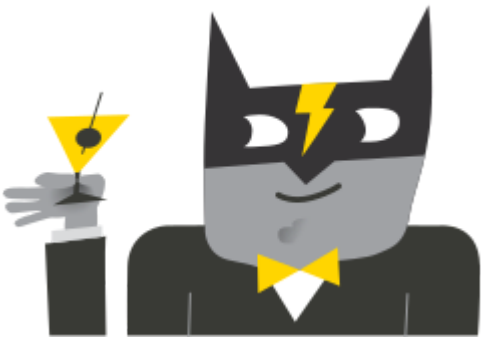
Tails is safer than any regular operating system. But Tails, or any software or operating system, cannot protect you from everything—even if they pretend to.

The recommendations below will keep you even safer, especially if you are at high risk.

Protecting your identity when using Tails

Tails is designed to hide your identity.

But some of your activities could reveal your identity:



- Sharing files with metadata, such as date, time, location, and device information
- Using Tails for more than one purpose at a time

Limitations of the Tor network

Tails uses the Tor network because it is the strongest and most popular network to protect from surveillance and censorship.

But Tor has limitations if you are concerned about:

- Hiding that you are using Tor and Tails
- Protecting your online communications from determined, skilled attackers

Reducing risks when using untrusted computers

Tails can safely run on a computer that has a virus.

But Tails cannot always protect you when:

- Installing from an infected computer
- Running Tails on a computer with a compromised BIOS, firmware, or hardware

Protecting your identity

Clean metadata from files before sharing them

Many files contain hidden data, or metadata:

- JPEG and other image files often contain information about where a picture was taken and which camera was used.
- Office documents often contain information about their author, and the date and time the document was created.

To help you clean metadata, Tails include *Metadata Cleaner*, a tool to remove metadata in a wide range of file formats.

Use Tails sessions for only one purpose at a time

If you use Tails sessions for more than one purpose at a time, an adversary could link your different activities together.

For example, if you log into different accounts on the same website in a single Tails session, the website could determine that the accounts are used by the same person. This is because websites can tell when 2 accounts are using the same Tor circuit.

To prevent an adversary from linking your activities together while using Tails, restart Tails between different activities. For example, restart Tails between checking your work email and your whistleblowing email.

We are not aware of any such attacks to deanonymize people online who used Tails for different purposes at a time.

If you worry that the files in your Persistent Storage could be used to link your activities together, consider using a different Tails USB stick for each activity. For example, use one Tails USB stick for your activism work and another one for your journalism work.

Limitations of Tor

Tails makes it clear that you are using Tor and probably Tails

Everything you do on the Internet from Tails goes through the Tor network.

Tor and Tails don't protect you by making you look like any random Internet user, but by making all Tor and Tails users look the same. It becomes impossible to know who is who among all users.

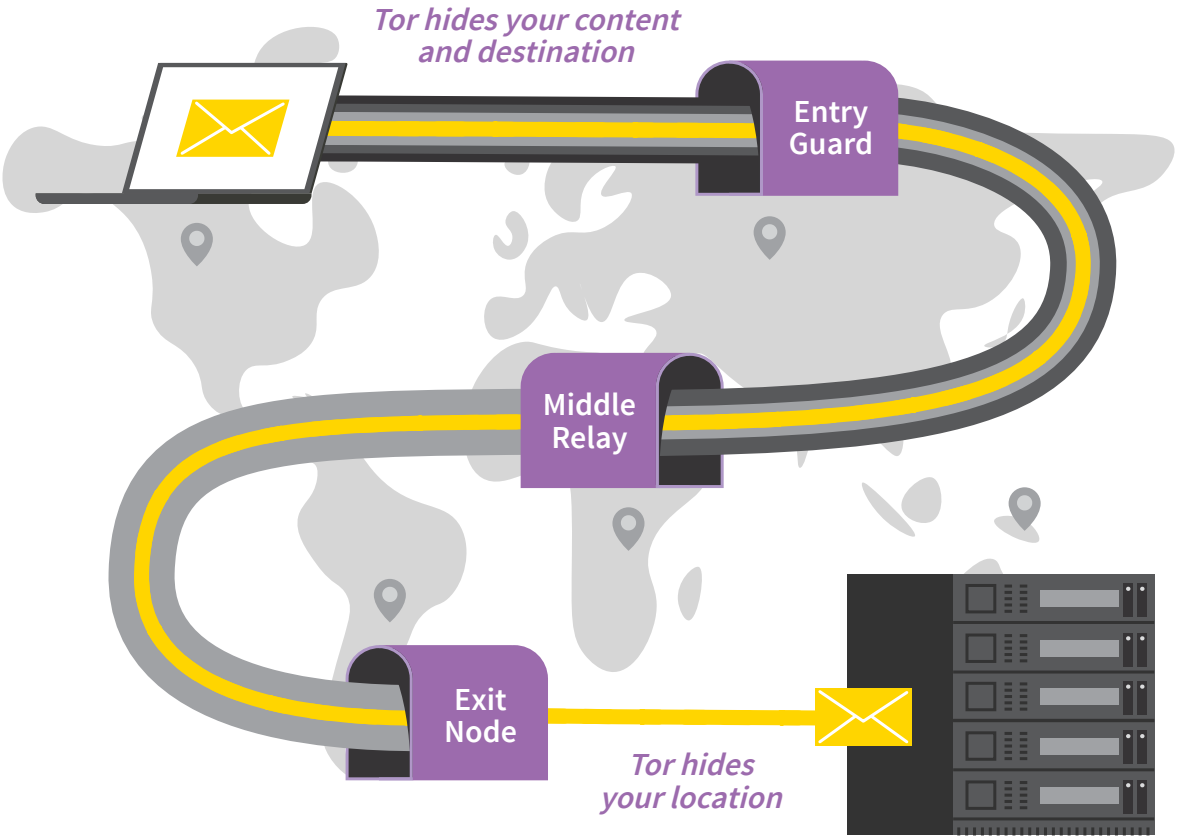
- Your Internet service provider (ISP) and local network can see that you connect to the Tor network. But, they cannot know which sites you visit. To also hide that you connect to Tor, use a Tor bridge.
- The sites that you visit can know that you are using Tor, because the list of exit nodes of the Tor network is public.

Parental controls, Internet service providers, and countries with heavy censorship can identify and block connections to the Tor network that don't use Tor bridges.

Many websites ask you to solve a CAPTCHA or block access from the Tor network.

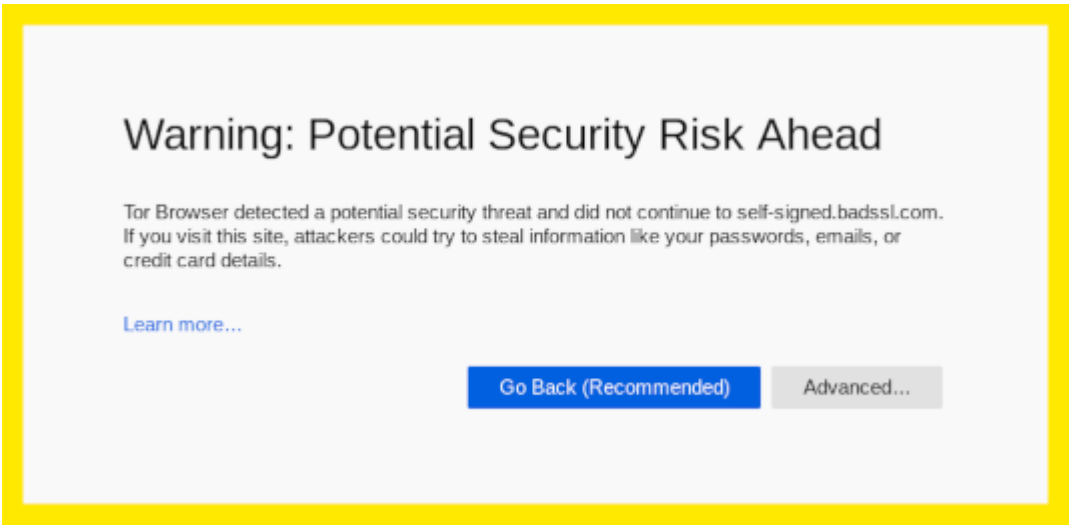
Exit nodes can intercept traffic to the destination server

Tor hides your location from destination servers, but it does not encrypt *all* your communication. The last relay of a Tor circuit, called the *exit node*, establishes the actual connection to the destination server. This last step can be unencrypted, for example, if you connect to a website using HTTP instead of HTTPS.



The exit node can:

- Observe your traffic. That is why *Tor Browser* and Tails include tools to encrypt the connection between the exit node and the destination server, whenever possible.
- Pretend to be the destination server, a technique known as *machine-in-the-middle* attack (MitM). That is why you should pay even more attention to the security warnings in *Tor Browser*. If you get such a warning, use the New Identity feature of *Tor Browser* to change exit node.


Warning: Potential Security Risk Ahead
Tor Browser detected a potential security threat and did not continue to self-signed.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...

To learn more about what information is available to someone observing the different parts of a Tor circuit, see the interactive graphics at Tor Support: How HTTPS encryption and Tor works in Tor Browser to enhance your privacy and anonymity.

Adversaries watching both ends of a Tor circuit could identify users

An adversary, who could control the 3 relays in a circuit, could deanonymize Tor users.

Tor chooses 3 relays that belong to 3 different network operators for each circuit.

Tails takes extra measures to use different circuits for different applications.

The Tor network has more than 6 000 relays. Organizations running Tor relays include universities like the MIT, activist groups like Riseup, nonprofits like Derechos Digitales, Internet hosting companies like Private Internet Access, and so on. The huge diversity of people and organizations running Tor relays makes it more secure and more sustainable.

A powerful adversary, who could analyze the timing and shape of the traffic entering and exiting the Tor network, might be able to deanonymize Tor users. These attacks are called *end-to-end correlation* attacks, because the attacker has to observe both ends of a Tor circuit at the same time.

No anonymity network used for rapid connections, like browsing the web or instant messaging, can protect 100% from end-to-end correlation attacks. In this case, VPNs (Virtual Private Networks) are less secure than Tor, because they do not use 3 independent relays.

Using untrusted computers

Install Tails from a computer that you trust

Tails protects you from viruses and malware on your usual operating system. This is because Tails runs independently from other operating systems.

But your Tails might be corrupted if you install from a compromised operating system. To reduce that risk:

- Always install Tails from a trusted operating system. For example, download Tails on a computer without viruses or clone Tails from a trusted friend.

- Do not plug in your Tails USB stick while another operating system is running on the computer.
- Use your Tails USB stick only to run Tails. Do not use your Tails USB stick to transfer files to or from another operating system.

If you worry that your Tails might be corrupted, do a manual upgrade from a trusted operating system.

We don't know of any virus able to infect a Tails installation, but one could be created in the future.

No operating system can protect against hardware alterations

The computer might be compromised if its physical components have been altered. For example, if a keylogger has been physically installed on the computer, your passwords, personal information, and other data typed on the keyboard could be stored and accessed by someone else, even if you are using Tails.

Try to keep your computer in a safe location. Hardware alterations are more likely on public computers, in Internet cafés or libraries, and on desktop computers, where a device is easier to hide.

If you worry that a computer might be modified:

- Use a password manager to paste saved passwords. This way, you don't have to type passwords that might be visible to people or cameras near you.
- Use the screen keyboard, if you are using a public computer or worry that the computer might have a keylogger.

No operating system can protect against BIOS and firmware attacks

Firmware includes the BIOS or UEFI and other software stored in electronic chips on the computer. All operating systems, including Tails, depend on firmware to start and run, so no operating system can protect against a firmware attack. In the same way that a car depends on the quality of the road it is driving on, operating systems depend on their firmware.

Keeping your computer in a safe location can protect against some firmware attacks, but some other firmware attacks can be performed remotely.

Download Tails

Save your download to your usual *Downloads* folder and not to the USB stick.

We recommend that you save your download to your Persistent Storage. Otherwise, Tails might stop responding if the RAM memory of the computer gets full.

While you are downloading, we recommend you read the release notes for Tails 7.10.1 . They document all the changes in this new version: new features, problems that were solved, and known issues that have already been identified.

Verify your download

Verify your download to make sure that it is safe and was not corrupted during download.

You seem to have JavaScript disabled. To verify your download, you can either:

- Enable JavaScript and reload this page.
- Compare manually the checksum of your download with the checksum of our images. In Tails, you can install *GtkHash* as Additional Software

- Verify your download using our OpenPGP signing key and OpenPGP signature. OpenPGP signature. We don't provide instructions to verify downloads with OpenPGP anymore.

  See our security analysis of the different verification techniques.

You seem to be using *Internet Explorer*. To verify your download, please use a different browser.

Select your download to verify…
or verify using the OpenPGP signature

OpenPGP signature OpenPGP signature

If you don't know how to use the OpenPGP signature, select instead the button **Select your download** to verify your download with JavaScript.

OpenPGP signing key

Security analysis of the different verification techniques

Verifying *$FILENAME*…

✔ **Verification successful!** (*$FILENAME*)

✖ **Verification failed!** (*$FILENAME*)

Why?

Most likely, the verification failed because of an error or interruption during the download.

The verification also fails if you try to verify a different download than the latest version, Tails 7.10.1 .

Less likely, the verification might have failed because of a malicious download from our download mirrors or due to a network attack in your country or local network.

Downloading again is usually enough to fix this problem. Otherwise, please try downloading from a different place or a different computer.

How does the verification work?

Please try to download again…

Please try to download again…

❌ **Error selecting image.**

Make sure that you select a USB image that is readable by your browser.

Make sure that you select an ISO image that is readable by your browser.

Retry…

❌ **Error downloading checksum file from our website.**

Make sure that your browser is connected to the Internet.

Retry…

❌ **Error reading image *$FILENAME*.**

Make sure that *$FILENAME* is readable by your browser.

Retry…

Download *Rufus*

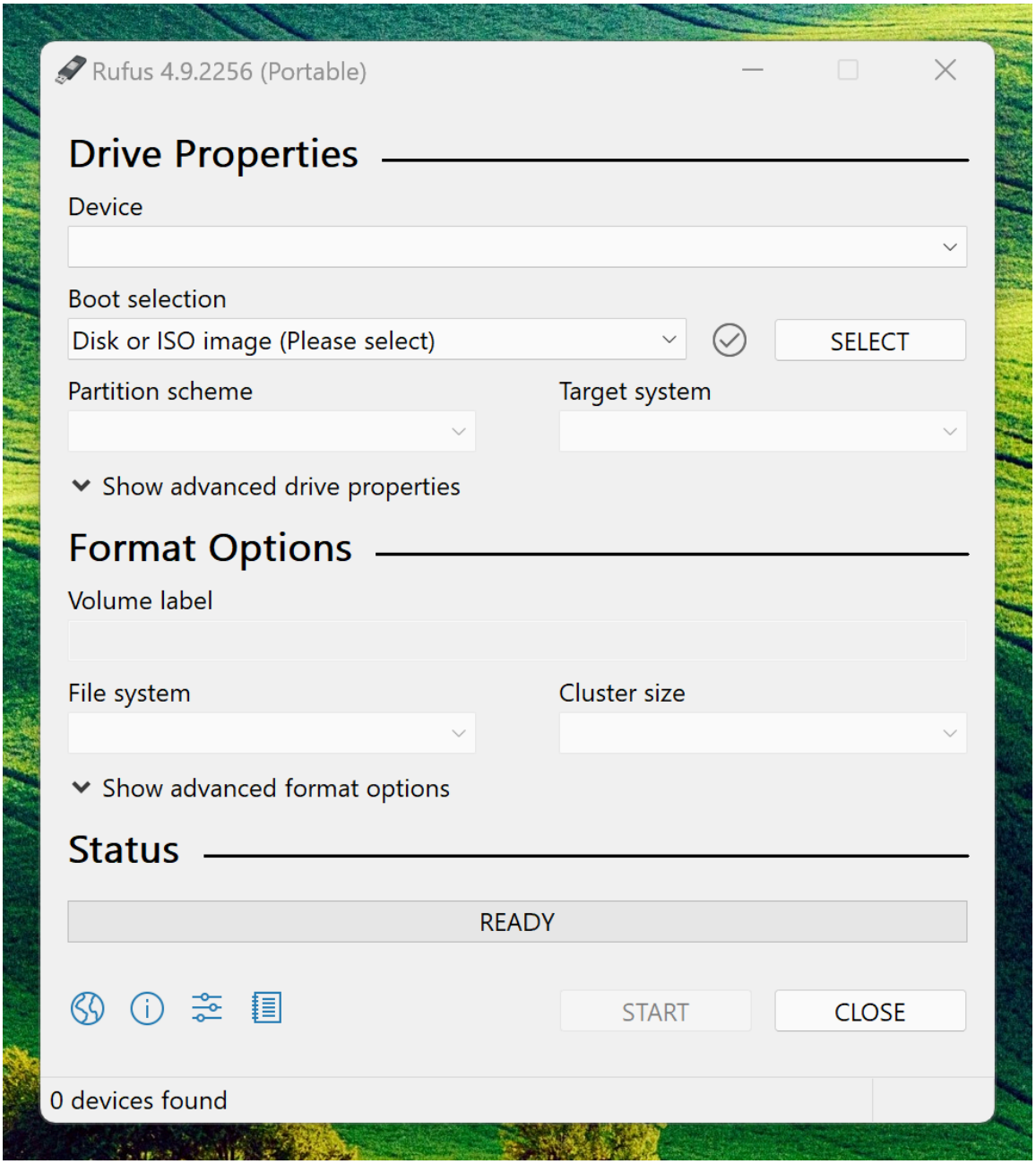
In the following steps, you will install an intermediary Tails using the Tails USB image that you downloaded earlier.

Rufus is the Free Software tool that we recommend to install Tails from Windows.

1. Click on the following button to download *Rufus*:

   Download *Rufus* for Windows

   Save your download to your usual *Downloads* folder and not to the USB stick.



3. Plug in the USB stick on which you want to install Tails. the intermediary Tails.

   All the data on this USB stick will be lost.

   Some data might still be recovered using advanced forensics tools.

   The Persistent Storage of your Tails USB stick will not be copied to the temporary Tails.

   Wait a few seconds until *Rufus* detects your USB stick.

4. Choose your USB stick in the **Device** menu.

   If your USB stick doesn't appear in the **Device** menu, make sure that you saved *Rufus* to your usual *Downloads* folder and not to the USB stick itself.

5. Click the **Select** button.

   Choose the USB image that you downloaded earlier.

   Make sure that the USB image is called *tails-amd64-7.10.1.img* and has an *.img* file extension.

   If the image has an *.iso* file extension, it is the wrong image. Please go back to the download step. download step.

6. Click **Start**.

   Enter your password if you are asked for it.

   The installation takes a few minutes.

7. Close *Rufus*.

   After installing Tails, the USB stick no longer appears in the *File Explorer* app of Windows.

   You can still see the USB stick in the *Settings* app. Choose **System ▸ Storage ▸ Advanced storage settings ▸ Disk & volumes**.

   See also how to uninstall Tails from Windows.

Well done!

You have installed Tails on your USB stick.

In the next step, you will make your computer start on this USB stick.

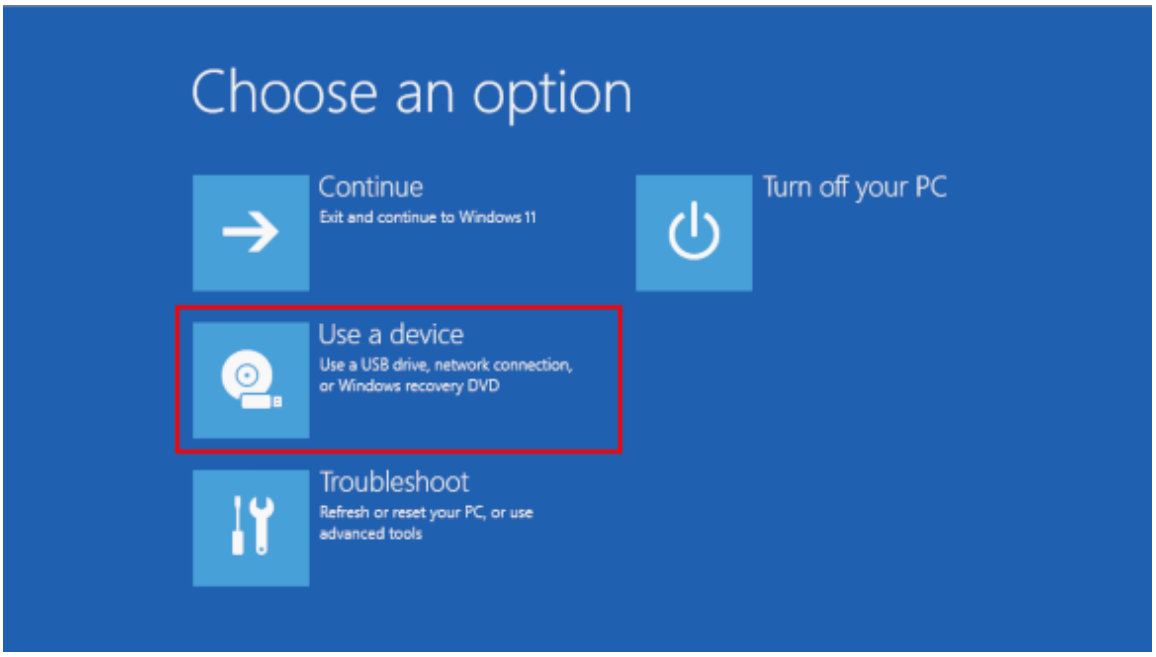
Tails might not work on your computer, so good luck!

If you already started on the other Tails, go directly to step 3: Verify that the other Tails is up-to-date.

3. Press and hold the **Shift** key while you select the **Power** button and then **Restart**.

   Windows shuts down and restarts on the **Choose an option** screen.

4. In the **Choose an option** screen, choose **Use a device**.


Choose an option
Continue
Exit and continue to Windows 11
Turn off your PC
Use a device
Use a USB drive, network connection, or Windows recovery DVD
Troubleshoot
Refresh or reset your PC, or use advanced tools

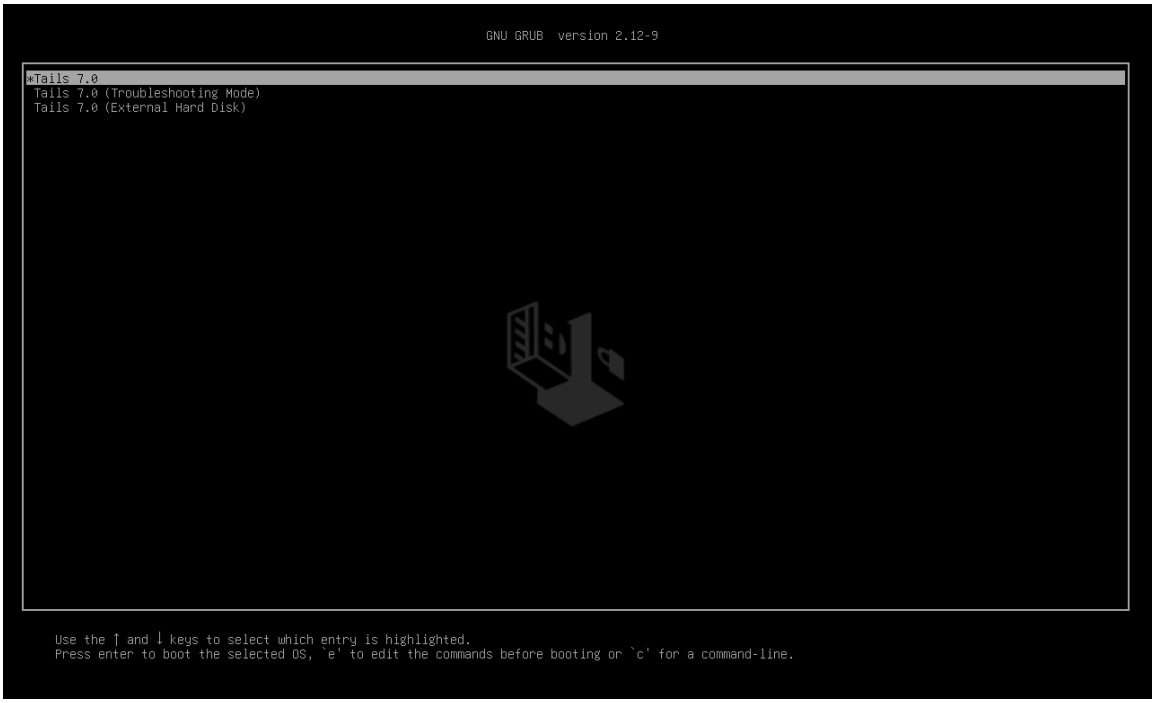
5. In the **Use a device** screen, select **USB HDD**.

   Windows shuts down and the computer restarts on your Tails USB stick.

   In the future, we We recommend that you only plug in your Tails USB stick while Windows is shutting down. Otherwise, a virus in Windows could infect your Tails USB stick and break its security.

   Such an attack is possible in theory but very unlikely in practice. We don't know of any virus capable of infecting Tails. See our warning on plugging Tails in untrusted systems.

6. If the computer starts on Tails, the Boot Loader appears and Tails starts automatically after 4 seconds.


GNU GRUB version 2.12-9
*Tails 7.0
Tails 7.0 (Troubleshooting Mode)
Tails 7.0 (External Hard Disk)
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.

   - The **Troubleshooting Mode** entry disables some features of the Linux kernel and might work better on some computers. You can try this option if you think you are experiencing hardware compatibility errors while starting Tails.

   - The **External Hard Disk** entry makes it possible to start from an external hard disk and some problematic USB sticks.

Most computers do not start automatically on the Tails USB stick, but you can press a Boot Menu key to display a list of possible devices to start from.

The following screenshot is an example of a Boot Menu:

This animation summarizes how to use the Boot Menu key to start on the USB stick:

The following instructions explain in detail how to use the Boot Menu key to start on the USB stick:

1. Make sure that you have installed Tails using either:

   - *Rufus* from Windows
   - *balenaEtcher* from macOS
   - *GNOME Disks* from Linux
   - the Linux command line

2. Shut down the computer while leaving the USB stick plugged in.

   Shut down the computer and plug in the Tails USB stick.

   Shut down the computer.

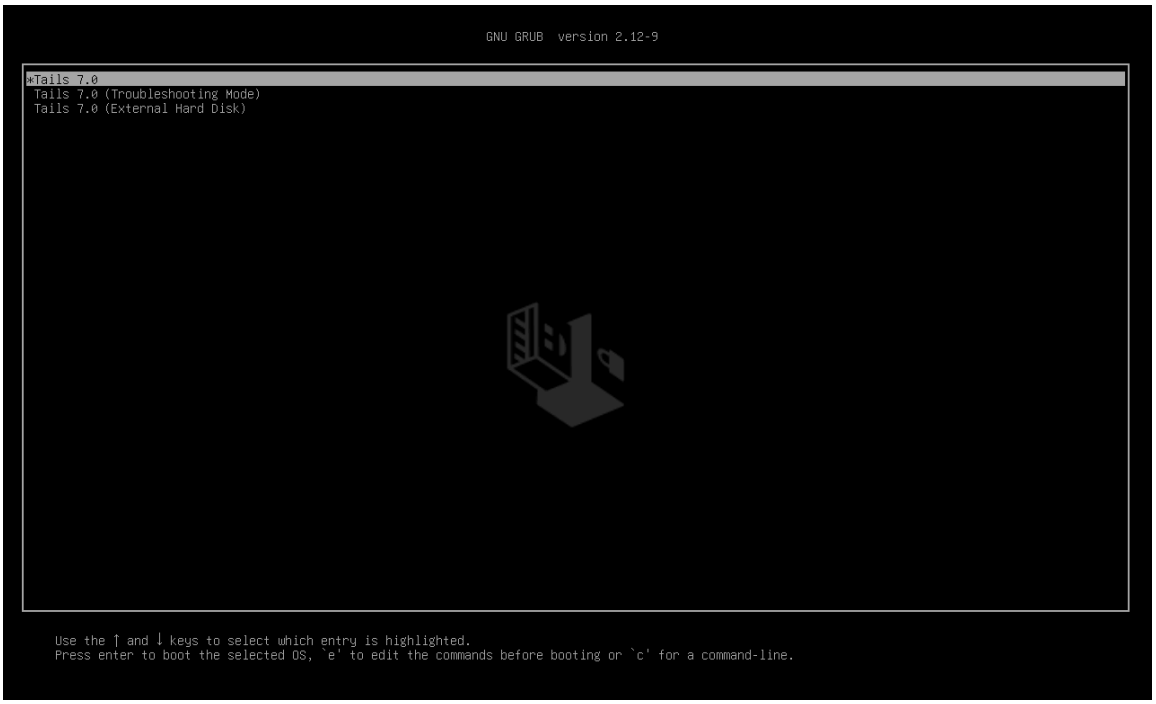
   Plug in the other Tails USB stick that you want to install upgrade from.

   Unplug your Tails USB stick while leaving the intermediary USB stick plugged in.

5. If the computer starts on another operating system or returns an error message, shut down the computer again and repeat step 3 for all the possible Boot Menu keys identified in step 2.

   If a Boot Menu with a list of devices appears, select your USB stick and press **Enter**.

6. If the computer starts on Tails, the Boot Loader appears and Tails starts automatically after 4 seconds.


GNU GRUB version 2.12-9
*Tails 7.0
Tails 7.0 (Troubleshooting Mode)
Tails 7.0 (External Hard Disk)
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.

0:00 / 0:37

1. Make sure that you have installed Tails using either:

    - *balenaEtcher* from macOS
    - *Rufus* from Windows
    - *GNOME Disks* from Linux
    - the Linux command line
2. Shut down the computer.

    Shut down the computer while leaving the USB stick plugged in.

    Plug in the other Tails USB stick that you want to install from.

3. Plug in your Tails USB stick.

4. Switch on the computer.

    Immediately press-and-hold the **Option** key (⌥ or **Alt** key) when the startup sound is played.

    Hold the key pressed until a list of possible startup disks appears.

5. Choose the USB stick and press **Enter**. The USB stick appears as an external hard disk and might be labeled **EFI Boot** or **Windows** like in the following screenshot:

If the USB stick does not appear in the list of startup disks:

1. Wait 2–3 minutes and try again. Some USB sticks need some rest after installing.

2. Try all other USB ports on the computer. Some USB ports cannot be used to start from.

3. Make sure that you have installed Tails using either:

   - *Rufus* from Windows
   - *balenaEtcher* from macOS
   - *GNOME Disks* from Linux
   - the Linux command line

4. Make sure that you have verified your download of Tails.

5. Make sure that you have verified your download.

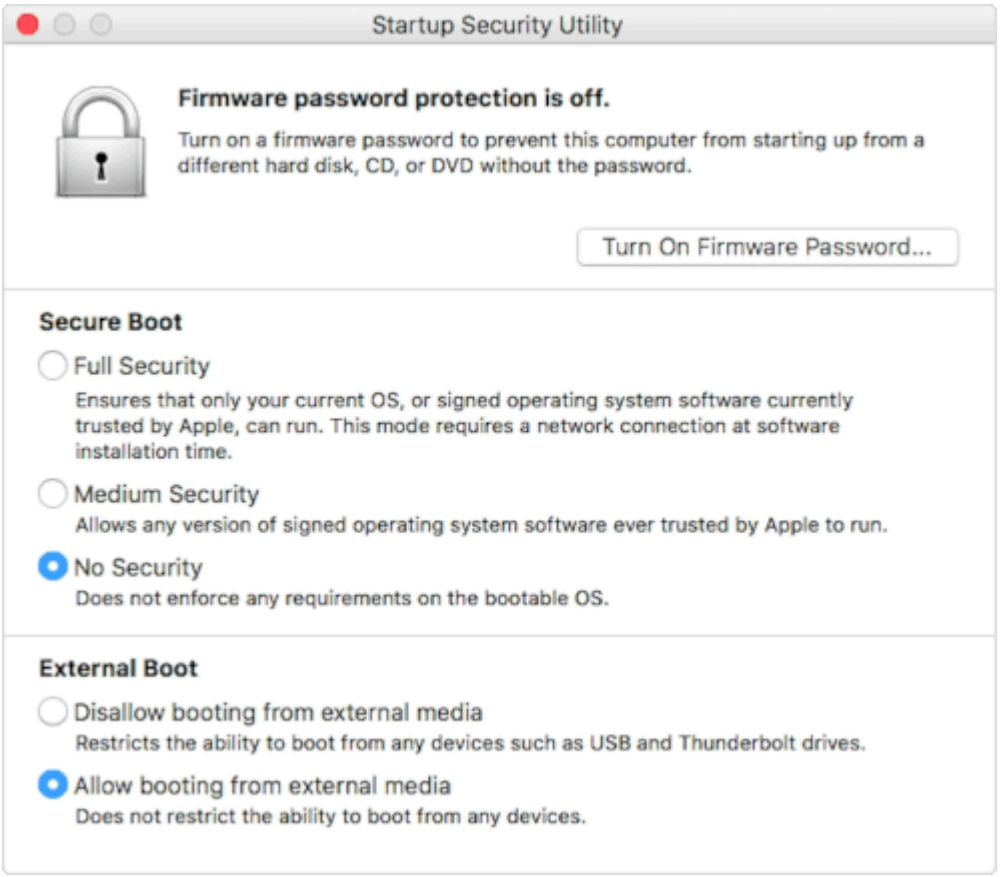
6. If your Mac displays the following error:

   Security settings do not allow this Mac to use an external startup disk.

   Then you have to change the settings of the *Startup Security Utility* of your Mac to authorize starting from Tails.

   To open *Startup Security Utility*:

   1. Turn on your Mac, then press and hold **Command(⌘)+R** immediately after you see the Apple logo. Your Mac starts up from macOS Recovery.
   2. When you see the macOS *Utilities* window, choose **Utilities ▸ Startup Security Utility** from the menu bar.
   3. When you are asked to authenticate, click **Enter macOS Password**, then choose an administrator account and enter its password.


Startup Security Utility
Firmware password protection is off.
Turn on a firmware password to prevent this computer from starting up from a different hard disk, CD, or DVD without the password.
Turn On Firmware Password...
Secure Boot
Full Security
Ensures that only your current OS, or signed operating system software currently trusted by Apple, can run. This mode requires a network connection at software installation time.
Medium Security
Allows any version of signed operating system software ever trusted by Apple to run.
No Security
Does not enforce any requirements on the bootable OS.
External Boot
Disallow booting from external media
Restricts the ability to boot from any devices such as USB and Thunderbolt drives.
Allow booting from external media
Does not restrict the ability to boot from any devices.

   In the *Startup Security Utility*:

   - Choose **No Security** in the **Secure Boot** section.
   - Choose **Allow booting from external media** in the **External Boot**.

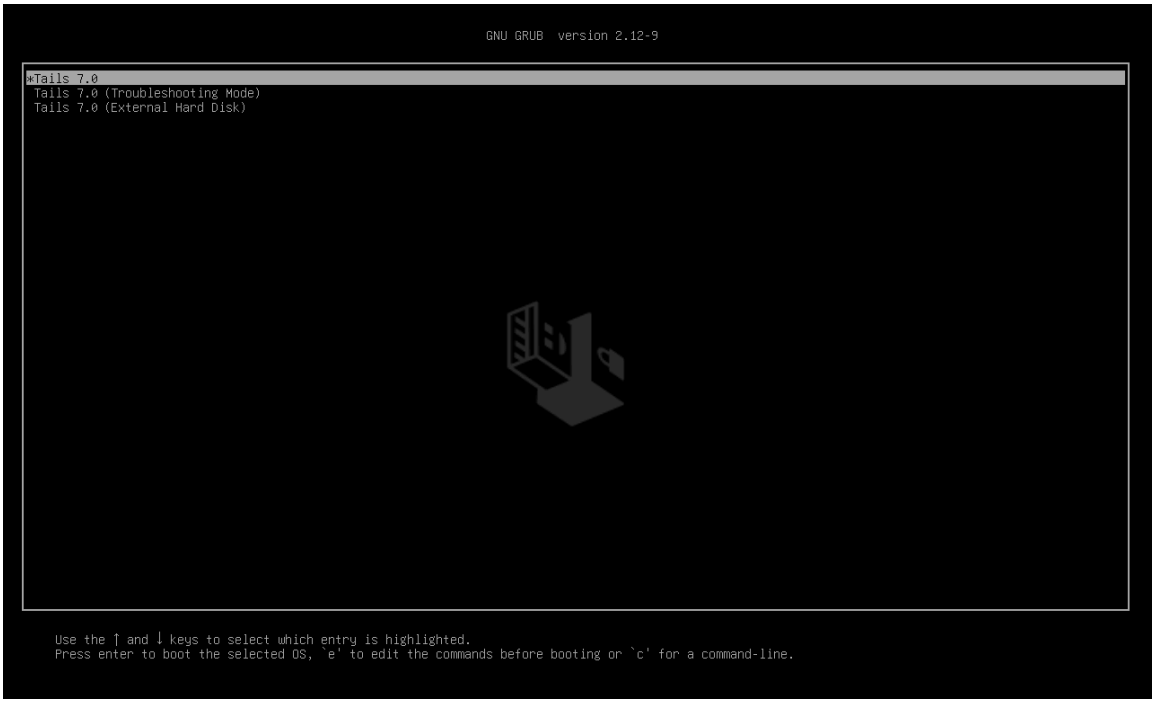
To still protect your Mac from starting on untrusted external media, you can set a firmware password, available on macOS Mountain Lion or later. A firmware password prevents users who do not have the password from starting up from any media other than the designated startup disk.

If you forget your firmware password you will require an in-person service appointment with an Apple Store or Apple Authorized Service Provider.

Read more on Apple Support about:

- Startup Security Utility
- How to set a firmware password on your Mac

7. If the computer starts on Tails, the Boot Loader appears and Tails starts automatically after 4 seconds.


GNU GRUB version 2.12-9
*Tails 7.0
Tails 7.0 (Troubleshooting Mode)
Tails 7.0 (External Hard Disk)
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.

   - The **Troubleshooting Mode** entry disables some features of the Linux kernel and might work better on some computers. You can try this option if you think you are experiencing hardware compatibility errors while starting Tails.

   - The **External Hard Disk** entry makes it possible to start from an external hard disk and some problematic USB sticks.

Troubleshoot Tails not starting

- If the computer doesn't restart on your Tails USB stick:

    1. Wait 2–3 minutes and try again. Some USB sticks need some rest after installing.

    2. Try other options in the **Use a device** screen, for example **USB FDD** if available.

    3. Try all other USB ports on the computer. Some USB ports cannot be used to start from.

    4. Refer to the instructions on starting Tails using the Boot Menu key.

- If none of the possible Boot Menu keys from the previous technique work, refer to the troubleshooting instructions about Tails not starting at all.

- If the Boot Menu appears, but your USB stick is not listed in the Boot Menu:

    1. Wait 2–3 minutes and try again. Some USB sticks need some rest after installing.

    2. Try all other USB ports on the computer. Some USB ports cannot be used to start from.

7. Try to install on a different USB stick.

8. Try to use the same USB stick to start on a different computer.

   If your computer still does not display the Boot Loader, it might currently be impossible to start Tails on your computer.

- If the Boot Loader appears, but Tails fails to start after the Boot Loader, refer to the troubleshooting section about Tails not starting after the Boot Loader. the troubleshooting section about Tails not starting after the Boot Loader.

Starting the computer using a Boot Menu key can be faster than starting the computer on Windows first and then on Tails. We recommend you learn how to start Tails using the Boot Menu key if you use Tails regularly.

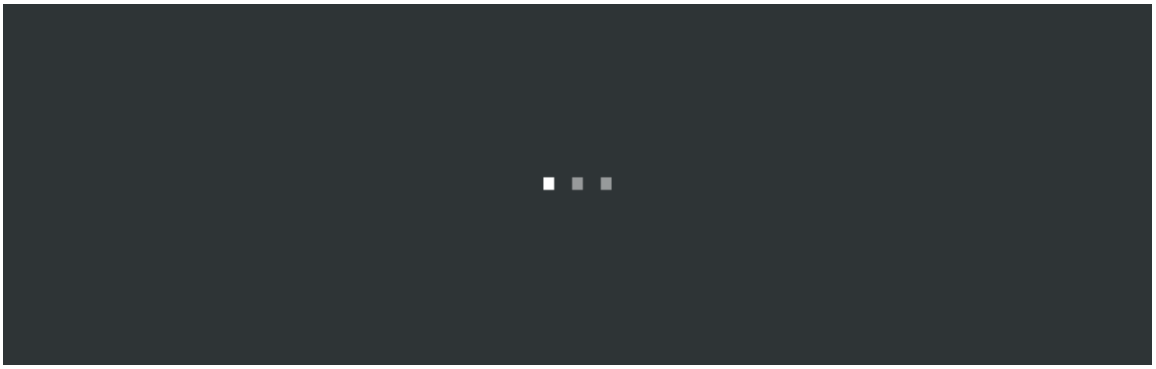
Apple does not prioritize collaborating with Free Software projects. Their newest hardware is usually very hard for Free Software developers to get working with Linux, and thus Tails. PC hardware tends to be more open and work better with Linux.

Welcome to Tails!

Starting the intermediary Tails

Starting the other Tails

1. After the Boot Menu, a loading screen appears.

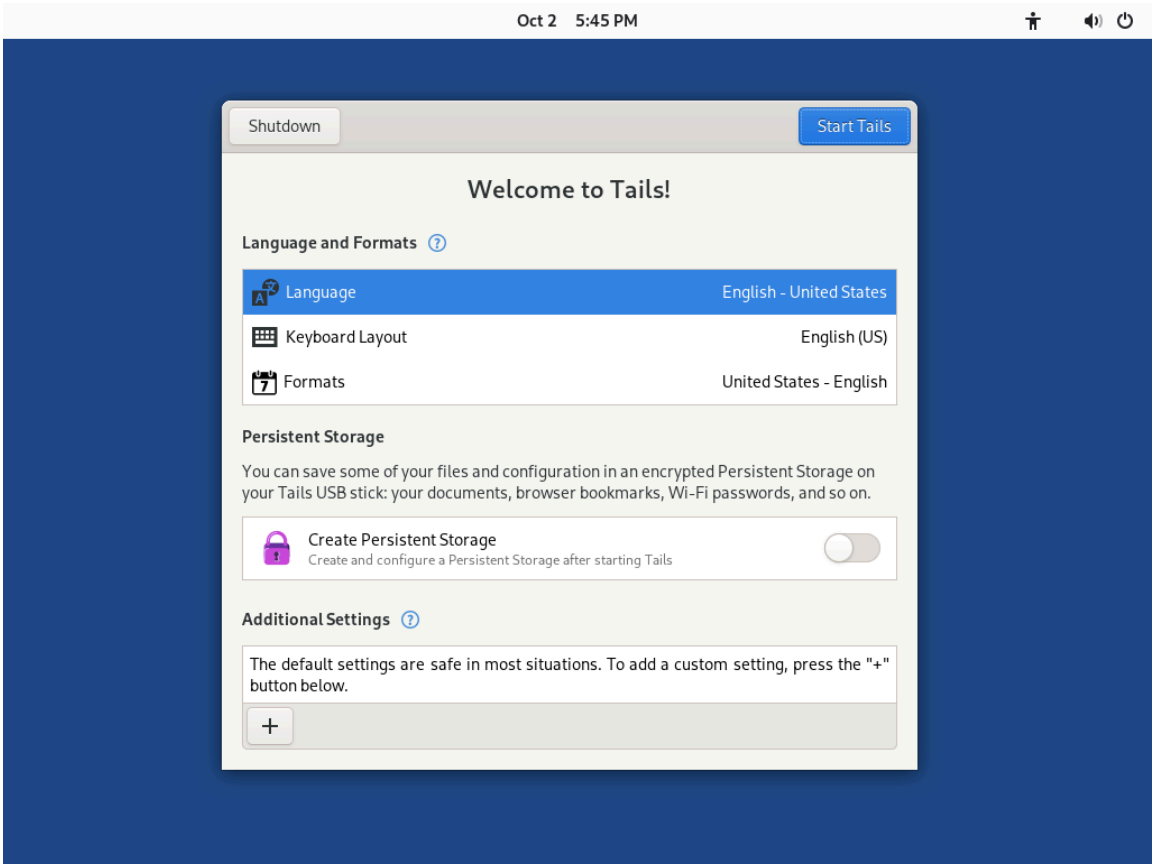


2. One to two minutes after the Boot Loader and the loading screen, the Welcome Screen appears.

   If the following message about partitioning errors appears in the Welcome Screen, please start again from step 2: Verify your download.

   Errors were detected in the partitioning of your Tails USB stick.

   If the error persists, reinstall Tails on one of our recommended USB sticks.


Oct 2 5:45 PM
Shutdown
Start Tails
Welcome to Tails!
Language and Formats
Language
English - United States
Keyboard Layout
English (US)
Formats
United States - English
Persistent Storage
You can save some of your files and configuration in an encrypted Persistent Storage on your Tails USB stick: your documents, browser bookmarks, Wi-Fi passwords, and so on.
Create Persistent Storage
Create and configure a Persistent Storage after starting Tails
Additional Settings
The default settings are safe in most situations. To add a custom setting, press the "+" button below.
+

3. In the Welcome Screen, select your language and keyboard layout in the **Language and Formats** section. Click **Start Tails**.

   If your keyboard or touchpad doesn't work, try using a USB keyboard or mouse.

4. After 15–30 seconds, the Tails desktop appears.

Welcome to your new Tails!

You made it!

You managed to start your new Tails on your computer!

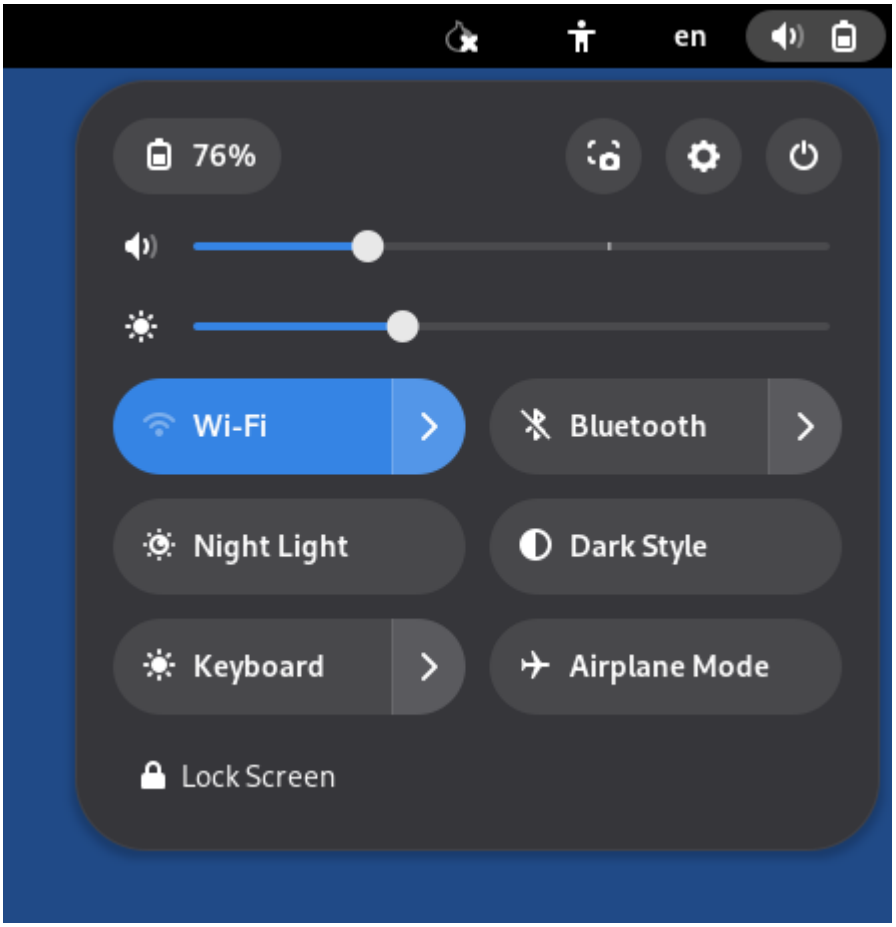
Congratulations on staying safe :)

To continue discovering Tails, read our documentation.

Test your Wi-Fi

Problems with Wi-Fi are unfortunately quite common in Tails and Linux in general. To test if your Wi-Fi interface works in Tails:

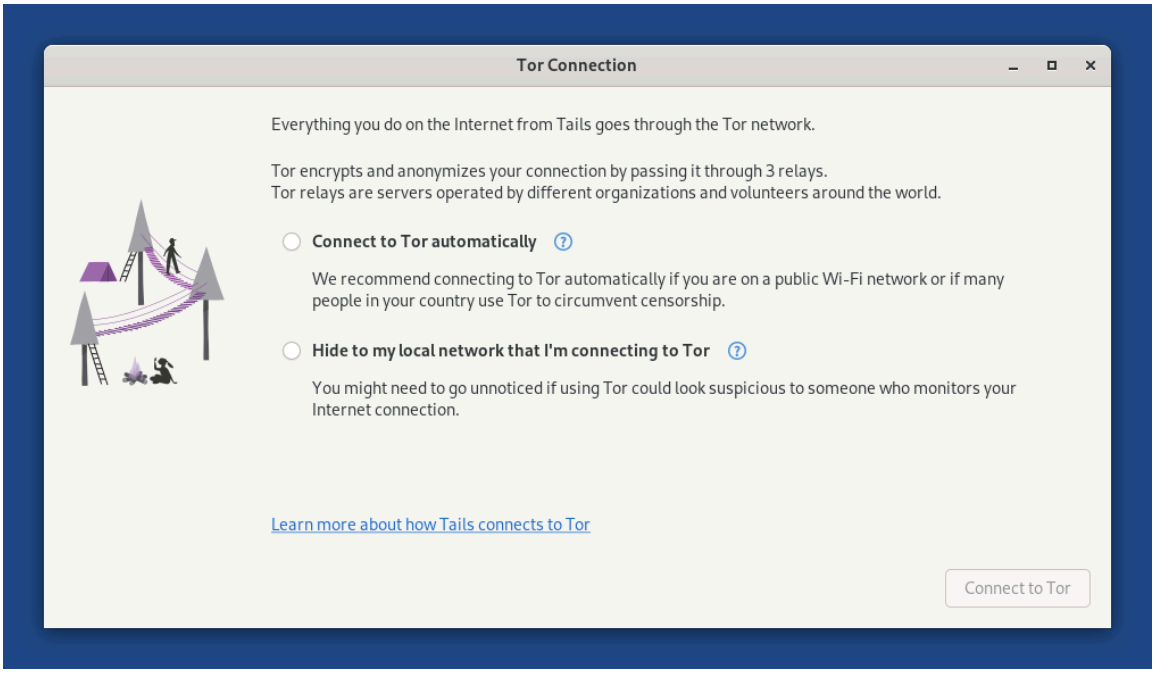
1. Open the system menu in the top-right corner:



2. Click › on the right of the **Wi-Fi** button.

   A list of available Wi-Fi networks appears below the **Wi-Fi** button.

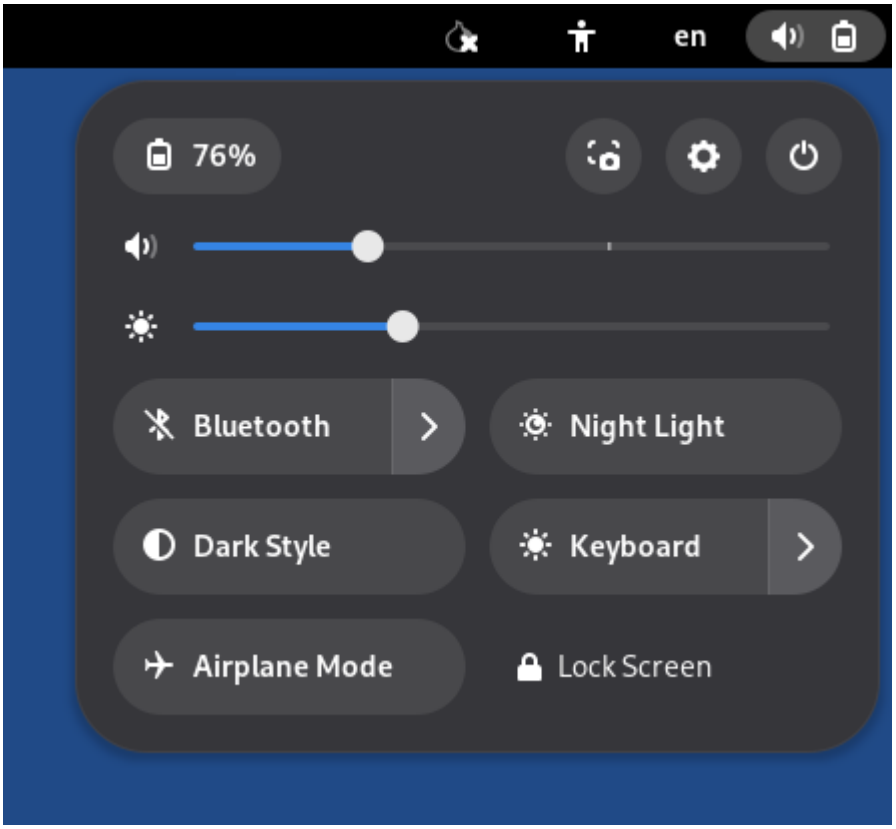
3. After establishing a connection to a local network, the *Tor Connection* assistant appears to help you connect to the Tor network.


Tor Connection
Everything you do on the Internet from Tails goes through the Tor network.
Tor encrypts and anonymizes your connection by passing it through 3 relays.
Tor relays are servers operated by different organizations and volunteers around the world.
Connect to Tor automatically
We recommend connecting to Tor automatically if you are on a public Wi-Fi network or if many people in your country use Tor to circumvent censorship.
Hide to my local network that I'm connecting to Tor
You might need to go unnoticed if using Tor could look suspicious to someone who monitors your Internet connection.
Learn more about how Tails connects to Tor
Connect to Tor

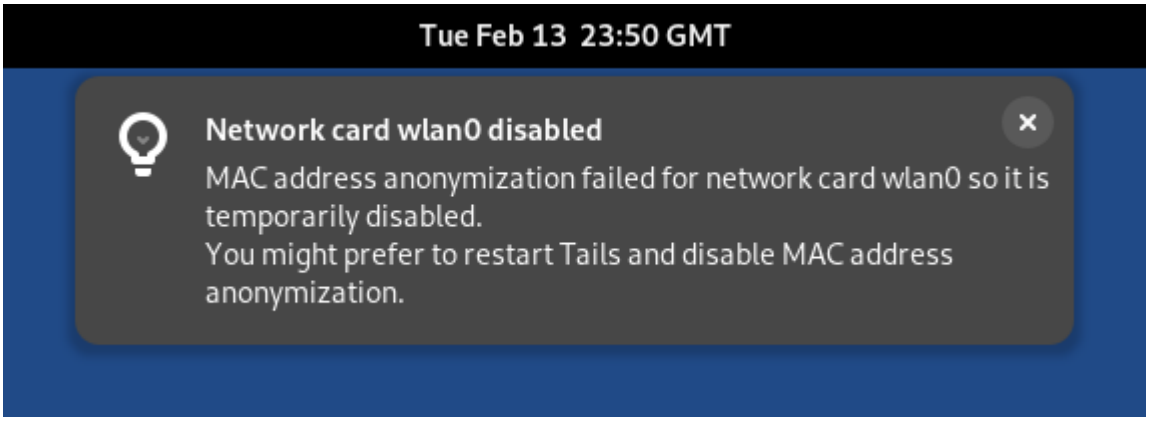
Troubleshooting Wi-Fi not working

If your Wi-Fi interface is not working, you might experience the following:

- There is no **Wi-Fi** menu in the system menu:



- There is a **Wi-Fi** menu in the system menu, but connecting to a Wi-Fi network fails.
- The interface is disabled because MAC address anonymization failed:


Tue Feb 13 23:50 GMT
Network card wlan0 disabled
MAC address anonymization failed for network card wlan0 so it is temporarily disabled.
You might prefer to restart Tails and disable MAC address anonymization.

  In this case, you can disable MAC address anonymization in the Welcome Screen. Doing so has security implications, so read carefully our documentation about MAC address anonymization.

- The following notification appears:

  ```
  Activation of network connection failed
  ```

To connect to the Internet, you can try to:

- Use an Ethernet cable instead of Wi-Fi if possible. Wired interfaces work much more reliably than Wi-Fi in Tails.

- Share the Wi-Fi or mobile data connection of your phone using a USB cable. Sharing a connection this way is called *USB tethering*.

  See instructions for:

  - iPhones or iPads

    Only sharing mobile data works on iPhones and iPads; sharing Wi-Fi does not work.

  - Android

  Tails cannot hide the information that identifies your phone on the local network. If you connect your phone to a:

  - Wi-Fi network: the network can see the MAC address of your phone.

    This has security implications that we explain in our documentation on MAC address anonymization. Some phones have a feature to hide the MAC address of the phone.

  - Mobile data network: the network is able to know the identifier of your SIM card (IMSI) and the serial number of your phone (IMEI).

  Buy a USB Wi-Fi adapter that works in Tails:

  - Panda Wireless Ultra ($25)

    Buy on Amazon

  - ThinkPenguin TPE-N150USB ($64)

    Buy on ThinkPenguin

  Check in our list of known Wi-Fi issues if there is a workaround to get your Wi-Fi interface to work in Tails.